【補助事業概要の広報資料】

補助事業番号　　24-84
補助事業名　　平成24年度　ＩｄＭにおける共通本人認証基盤の開発研究補助事業
補助事業者名　　一般社団法人　日本自動認識システム協会

１　補助事業の概要

（１）事業の目的

今後の電子サービス等の充実に伴い、複数のサービスを跨るＩｄＭ(アイデンティティマネジメント)システムにおいてサービスをより安全で安心な形で提供することが必要になることが予想される。パスワードに代わるより強固なセキュリティ性を提供するため、ＩｄＭシステムにバイオメトリクスを組み込むことを可能とする本人認証基盤の研究、開発とその評価を行った

（２）実施内容

①　ＩｄＭにおける共通本人認証基盤の開発研究
(http://www.bsc-japan.com/pdf/20130415/20130415-multimodal.pdf)

欧米諸国のIdMに関する最新の技術動向や標準化の動向と電子認証におけるセキュリティの考え方との整合性に関する調査を実施し、IdMにバイオメトリック認証を組み込むための知見を得た。また、OpenIDインタフェースを持つIdMシステムを選択し、そのIdMシステムにバイオメトリック技術を実装する共通バイオメトリック認証基盤の仕様を検討の上、プロトタイプソフトウェアを開発し、その動作を確認した。

なお実施にあたって、産官学の有識者により構成した委員会(ＩｄＭにおける共通本人認証基盤検討委員会)(産:委員９名、オブザーバ４名、官:オブザーバ２名、学:委員２名)を構成し、関連調査、開発仕様の開発とまとめ、並びにプログラム開発内容の検証作業の確認を行った。

概要は下記である。

1) 共通バイオメトリック認証基盤ソフトウェアの研究、開発

① 関連技術の最新動向調査

昨年に引き続き10月下旬に開催された英国Biometrics Exhibition and Conference 2012の調査を行い、訪米の社会的（ID関係の実証プロジェクト、脆弱性プライバシーなどの）プロジェクトの状況を調査した。

相変わらず欧米は日本よりはるかに進んでいるが、技術開発的には日本の企業の方が遥かに進んでいるようであったが、欧州は、アフリカ、中近東などの国へのバイオメトリクスを市場展開することに重点を置いて取り組んでいるようであった。日本において社会的な大型プロジェクトが実施されていないことやアジアへの市場展開が遅いことが、日本の産業界の問題との認識を持った。

② 電子認証におけるセキュリティの考え方との整合性に関する調査

電子認証システム関連規格調査およびセキュリティの考え方の整理として、米国の電子認証システムのための本人認証に関するガイドラインであるOMB M-04-04およびNIST SP 800-63について調査を行った。

その結果、電子認証システムにおける本人認証の保証レベルが1から4までの4段階で定義される中で、ハードウェアトークン・ソフトウェアトークン・パスワードなどの既存の本人認証技術を用いることで達成される保証レベルに対して、生体認証技術はその保証レベルを引き上げる役割を与えられていることが分った。

次に、電子認証システム等のセキュリティの考え方に対応するための要件の研究として、OpenIDと生体認証を組み合わせたシステム要件について検討した。

その結果、現在広く普及しているOpenIDシステムが比較的低い保証レベルで使われるケースが主流であるのに対して、電子認証システムのための本人認証ガイドラインにおいては生体認証技術の位置づけがより高い保証レベルを実現するものとして捉えられていることがわかった。

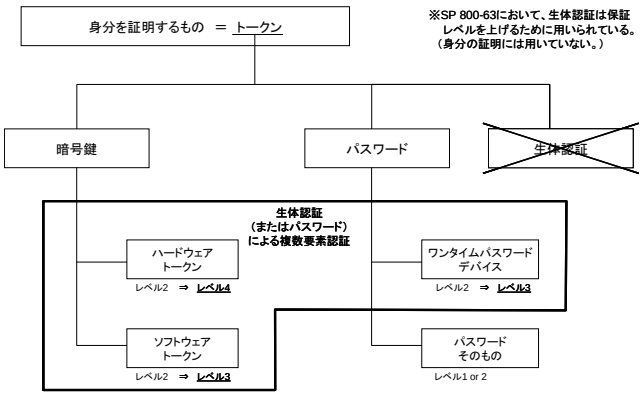

図1 SP 600-83における生体認証技術の位置づけ

保証レベルの不一致を避けることができるシステム要件を検討した結果、震災時の電子認証システムを取り上げることができた。震災時における利用環境を考えると、ハードウェアトークン・ソフトウェアトークン・パスワードのいずれも、電子認証システムにおける本人認証として被災者に適用するには困難さが存在するが、生体認証は簡便さと高セキュリティという2つの特長に加えて、紛失・盗難の恐れがなく、また記憶する必要もないため、震災時において広範囲な被災者への適用が可能であると考えられるためである。

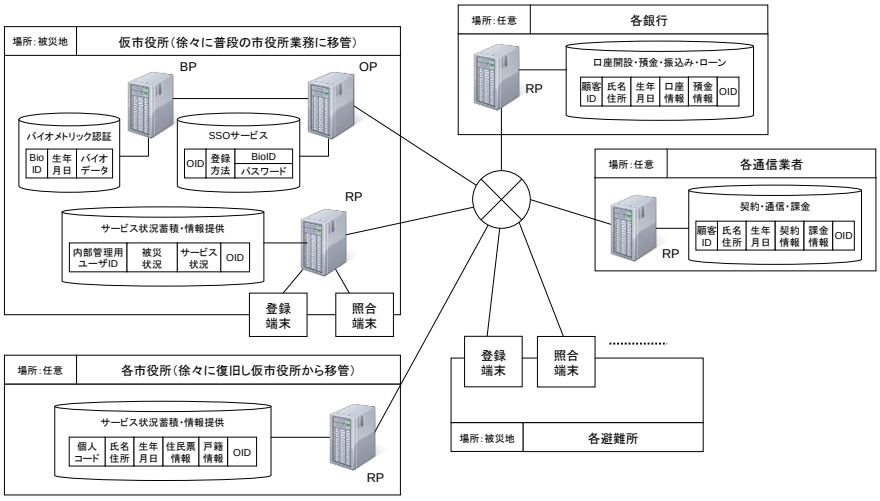

図2 震災時のOpenIDと生体認証を組み合わせた適用案

③ 共通バイオメトリック認証基盤の仕様検討

共通バイオメトリック認証基盤として共通本人認証基盤（BioIDMシステムと称する）に関する仕様検討を行った。

BioIDMシステムのシステム構成として、運用上標準的に用いられることを想定した標準構成(OP(OpenID Provider)、BP(BioIDM Provider)(バイオメトリック認証の機能を提供するもの)が独立している構成)と構造がより単純な簡易構成(OP(OpenID Provider)、BP(BioIDM Provider)が一体になった構成)の2種類を検討し、両構成の処理の流れ、長所と短所を明確にした。

標準構成における処理の流れについては開発効率を考慮し、OP・BP・UA(User Agent)間のプロトコルとしてOpenIDプロトコルを採用することとした。認証方式としてはサーバ認証に比べてセキュリティ対策の条件が緩やかなローカル認証方式を採用することとした。

サーバ側で動作するプログラムとしてOPにおけるBPとの連携機能、BPにおけるOPとの連携機能およびバイオメトリック登録・認証機能の仕様検討を行い、また、端末側で動作するプログラムとして、前年度開発のBioIDM Connectionと

BioIDM Transactionにおける登録・照合機能の仕様検討を行った。

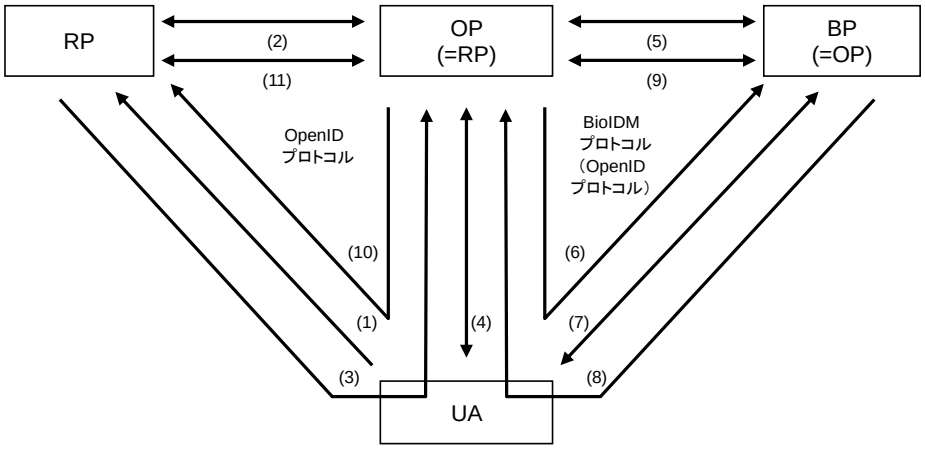

図3 BioIDMシステム標準構成における認証処理の流れ

また、以上の仕様検討結果を受けて、OpenIDプロバイダを用いるプロトタイプシステムの開発仕様を明確にした。

プロトタイプシステムの開発においては、OpenIDプロバイダとしてWSO2社のオープンソースであるIdentity Server 4.0版を使用し、生体認証装置としては日立製作所の指静脈認証装置PC-KCA100を用いたプロトタイプシステムを開発することとした。

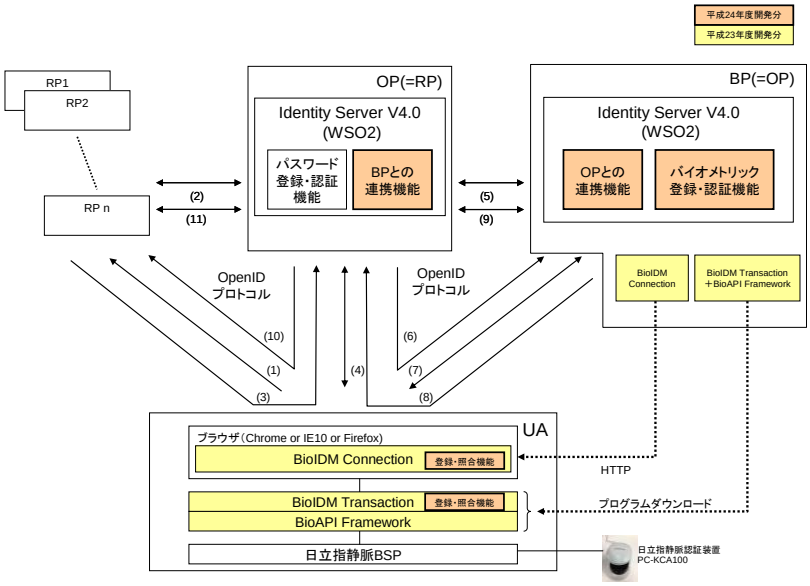

図 4 プロトタイプシステム構成図

2) 開発システムの検証実験と評価

共通バイオメトリック認証基盤の仕様検討結果に沿って開発したBioIDMシステムのプロトタイププログラムについて、その機能や性能の有効性を検証するために、実行環境の要素を変化させながら様々な環境でBioIDMシステムの検証実験を行った。検証実験の成果を下記に示す。

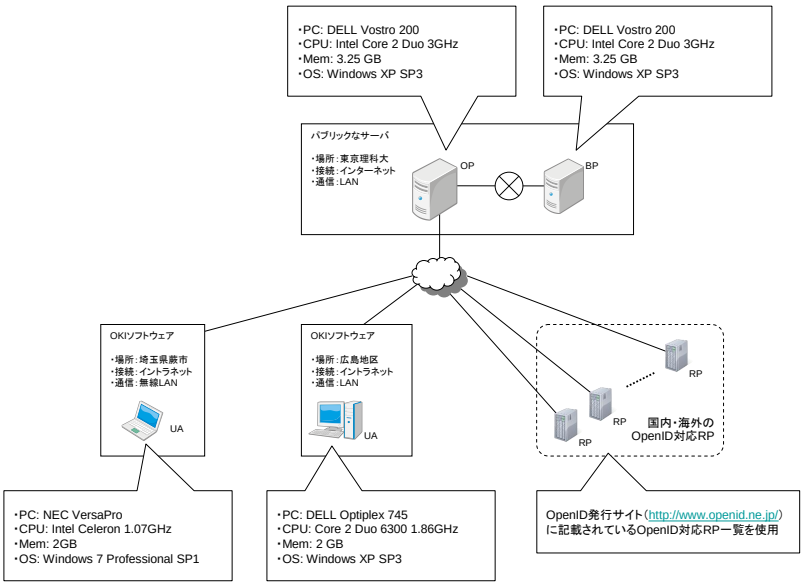

図5 検証実験のシステム構成図

①基本条件試験および簡易構成試験

WSO2のIdentity ServerとBioIDMシステム（BioIDM Connection、BioIDM Transaction、BioAPI Framework）および日立指静脈認証装置を組み合わせることにより、バイオメトリック認証を用いたOpenIDシステムのバイオメトリック情報登録から認証までの基本機能およびSSOの機能が正常に動作することを確認できた。

②性能測定

標準構成と簡易構成の2種類の構成で、バイオメトリック認証に要する時間を計測した。特に標準構成においてOPとBPの間の通信処理時間が大きく、簡易構成の約2倍の時間がかかっていることがわかった。RP(Relying Party)やOP(OpenID Provider)・UA(User Agent)などの各構成要素間のOpenIDプロトコルのための通信回数が多く、その分時間を要したことが標準構成において時間がかかる原因と考えられる。

③ブラウザとSSL

WebSocketは主要ブラウザへの搭載が出揃ったばかりの比較的新しい技術であるが、Google Chrome・Internet Explorer 10(Windows7 Prerelease版)、FirefoxともにBioIDM TransactionとのWebSocket通信が正常に動作することが確認でき

た。ただし、BioIDM Transactionに組み込んだWebSocketにおいて現状SSLが実現されておらず、セキュリティ上の問題となるとともに、Internet Explorer 10やFirefoxではWebサーバがHTTPSで動作している場合、WebSocketがSSL未サポートだと通信が失敗してしまうことがわかった。

④国内・海外RP接続

国内RP、海外RPともに今回開発したBioIDMシステムの標準構成にてバイオメトリック認証による正常なログオンが行えることがわかった。ただし、一部のRPについて正常動作しなかった。いくつかのケースにおいてOPに対してOpenIDプロトコルが通知されてこないことから、RPが利用可能なOPを限定している可能性が考えられる。

２　予想される事業実施効果

ＩｄＭ技術とバイオメトリック認証技術を標準的に組み合わせたケースは世界的に存在せず、また、そのための規格も存在していない。

本事業は、ＩｄＭおよびバイオメトリクス関係の国際標準に則し、新技術の国際標準化を目指して新技術の開発を行い、また成果も業界関係者で共有する予定で進めており、技術の適用先は日本国内だけでなく、海外への適用も可能である。

したがって、開発成果は、日本国内だけでなく海外のシステムへ適用するもことも考えられる。このため、事業成果の適用先が拡大し、国内産業の市場が海外へも広がることに寄与できると考えている。

３　本事業により作成した印刷物等

平成24年度　IdMにおける共通本人認証基盤の開発研究報告書

(http://www.bsc-japan.com/pdf/20130415/20130415-multimodal.pdf)

４　事業内容についての問い合わせ先

団 体 名：　(一社)日本自動認識システム協会（ﾆﾎﾝｼﾞﾄﾞｳﾆﾝｼｷｼｽﾃﾑｷｮｳｶｲ）
住　　所：　〒101-0032
東京都千代田区岩本町1-9-5 FKビル7F
代 表 者：　代表理事　会長　　土橋　郁夫（ドバシ　イクオ）
担当部署：　開発センター（カイハツセンター）
担当者名：　主任研究員　酒井　康夫（サカイ　ヤスオ）
電話番号：　03-5825-6651(代表)
ＦＡＸ：　　03-5825-6653
E-mail：　　y-sakai@jaisa.or.jp
ＵＲＬ　：　http://www.jaisa.jp/